

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, L.L.P.

1300 I STREET, N. W.  
WASHINGTON, DC 20005-3315

202 • 408 • 4000  
FACSIMILE 202 • 408 • 4400

ATLANTA  
404 • 653 • 6400  
PALO ALTO  
650 • 849 • 6600

WRITER'S DIRECT DIAL NUMBER:

(202) 408-4024

March 3, 2000

TOKYO  
011 • 813 • 3431 • 6943  
BRUSSELS  
011 • 322 • 646 • 0353

ATTORNEY DOCKET NO.: 04329.2244

**Box Patent Application**  
**Assistant Commissioner for Patents**  
**Washington, D.C. 20231**

New U.S. Patent Application

Title: CRYPTOGRAPHIC COMMUNICATION TERMINAL, CRYPTOGRAPHIC  
COMMUNICATION CENTER APPARATUS, CRYPTOGRAPHIC  
COMMUNICATION SYSTEM, AND STORAGE MEDIUM

Inventors and Addresses:

Kouya TOCHIKUBO  
Yokohama-shi, Japan

Naoki ENDOH  
Fuchu-shi, Japan

Sir:

We enclose the following papers for filing in the United States Patent and  
Trademark Office in connection with the above patent application.

1. A check for \$708 representing the filing fee.
2. Application - 47 pages, including 2 independent claims and 21 claims total.
3. Drawings - 6 sheets of formal drawings containing 7 figures.
4. Certified copy of Japanese Application No. 11-058592, filed March 5, 1999.



X 4

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER, L.L.P.

Assistant Commissioner for Patents

March 3, 2000

Page 2

This application is being filed under the provisions of 37 C.F.R. § 1.53(f). Applicants await notification from the Patent and Trademark Office of the time set for filing the Declaration.

Applicants claim the right to priority based on Japanese Application No. 11-058592, filed March 5, 1999.

Please accord this application a serial number and filing date.

The Commissioner is hereby authorized to charge any additional filing fees due and any other fees due under 37 C.F.R. § 1.16 or § 1.17 during the pendency of this application to our Deposit Account No. 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,  
GARRETT & DUNNER, L.L.P.

By: 

Richard V. Burgujian  
Reg. No. 31,744

RVB/FPD/dvz  
Enclosures

日 本 国 特 許 庁  
PATENT OFFICE  
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日

Date of Application:

1999年 3月 5日

出 願 番 号

Application Number:

平成11年特許願第058592号

出 願 人

Applicant (s):

株式会社東芝

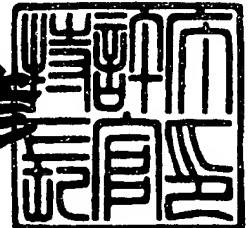
jc713 U.S. PTO  
09/518782  
03/03/00

CERTIFIED COPY OF  
PRIORITY DOCUMENT

2000年 1月28日

特許庁長官  
Commissioner,  
Patent Office

近藤 隆彦



【書類名】 特許願

【整理番号】 A009900214

【提出日】 平成11年 3月 5日

【あて先】 特許庁長官 殿

【国際特許分類】 H04L 12/00  
G06F 7/00

【発明の名称】 暗号通信端末、暗号通信センター装置、暗号通信システム及び記憶媒体

【請求項の数】 17

【発明者】

    【住所又は居所】 東京都府中市東芝町 1 番地 株式会社東芝府中工場内

    【氏名】 枡窪 孝也

【発明者】

    【住所又は居所】 東京都府中市東芝町 1 番地 株式会社東芝府中工場内

    【氏名】 遠藤 直樹

【特許出願人】

    【識別番号】 000003078

    【氏名又は名称】 株式会社 東芝

【代理人】

    【識別番号】 100058479

    【弁理士】

    【氏名又は名称】 鈴江 武彦

    【電話番号】 03-3502-3181

【選任した代理人】

    【識別番号】 100084618

    【弁理士】

    【氏名又は名称】 村松 貞男

【選任した代理人】

    【識別番号】 100068814

【弁理士】

【氏名又は名称】 坪井 淳

【選任した代理人】

【識別番号】 100092196

【弁理士】

【氏名又は名称】 橋本 良郎

【選任した代理人】

【識別番号】 100091351

【弁理士】

【氏名又は名称】 河野 哲

【選任した代理人】

【識別番号】 100088683

【弁理士】

【氏名又は名称】 中村 誠

【選任した代理人】

【識別番号】 100070437

【弁理士】

【氏名又は名称】 河井 将次

【手数料の表示】

【予納台帳番号】 011567

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 暗号通信端末、暗号通信センター装置、暗号通信システム  
及び記憶媒体

【特許請求の範囲】

【請求項 1】 暗号通信における情報送受信の一方となる暗号通信端末において、

前記暗号通信に用いる暗号アルゴリズムを 1 種類以上格納するとともに、指定された暗号アルゴリズムを出力する暗号アルゴリズム格納部と、

前記暗号アルゴリズムに対応した暗号通信用の鍵を格納するとともに、指定された鍵を出力する鍵情報格納部と、

前記暗号通信において何れの暗号アルゴリズム及び鍵を使用するかを、前記暗号アルゴリズム格納部及び前記鍵情報格納部に対してそれぞれ指定する制御手段と、

前記暗号アルゴリズム格納部に対して指定された暗号アルゴリズム及び前記鍵情報格納部に対して指定された鍵によって、受信した暗号情報を復号化し、又は、送信する情報を暗号化する暗号化・復号化手段とを備えたことを特徴とする暗号通信端末。

【請求項 2】 前記暗号アルゴリズム格納部は、暗号化された暗号アルゴリズムを格納するとともに、

前記暗号化された暗号アルゴリズムを復号化する暗号アルゴリズム復号化手段を備えたことを特徴とする請求項 1 記載の暗号通信端末。

【請求項 3】 前記鍵情報格納部は、前記暗号通信用の鍵の他、暗号化された暗号アルゴリズムを復号化する際に用いるアルゴリズム復号化鍵を格納することを特徴とする請求項 2 記載の暗号通信端末。

【請求項 4】 前記鍵情報格納部は、暗号化された鍵を格納するとともに、前記暗号化された鍵を復号化する鍵情報復号化手段を備えたことを特徴とする請求項 1 乃至 3 のうち何れか一項に記載の暗号通信端末。

【請求項 5】 前記制御手段は、前記暗号アルゴリズム格納部に格納する何れかの暗号アルゴリズムについての送信要求を受けた場合に、当該要求暗号アル

ゴリズムを出力するよう前記暗号アルゴリズム格納部に指令し、

前記暗号化・復号化手段は、前記要求暗号アルゴリズムを前記送信する情報として暗号化することを特徴とする請求項 1 乃至 4 のうち何れか一項に記載の暗号通信端末。

【請求項 6】 自己の通信相手が請求項 5 の暗号通信端末又は請求項 1 乃至 6 のうち何れか一項に記載の暗号通信端末を備える装置である場合に、当該通信相手に新たな暗号アルゴリズム及び又はこれに対応するアルゴリズム復号化鍵を要求し、その応答を暗号化・復号化手段にて復号化するとともに、

要求した暗号アルゴリズムを受け取った場合にはこれを前記暗号アルゴリズム格納部に格納し、要求したアルゴリズム復号鍵を受け取った場合にはこれを前記鍵情報格納部に格納することを特徴とする請求項 1 乃至 5 のうち何れか一項に記載の暗号通信端末。

【請求項 7】 前記請求項 1 乃至 6 のうち何れか一項に記載の暗号通信端末を備えるとともに、

通信相手から前記アルゴリズム復号化鍵を要求された場合には、該当するアルゴリズム復号化鍵を要求元への前記送信する情報として前記暗号化・復号化手段に入力することを特徴とする暗号通信センター装置。

【請求項 8】 前記請求項 5 記載の暗号通信端末を備える場合に、

前記アルゴリズム復号化鍵にて暗号化された暗号アルゴリズムを複数種類格納する更新用暗号アルゴリズム格納部を備え、

前記制御手段は、前記暗号通信端末から暗号アルゴリズムを要求された場合には、前記暗号アルゴリズム格納部に代え、前記更新用暗号アルゴリズム格納部に対して前記要求暗号アルゴリズムを前記送信する情報として出力するよう指令することを特徴とする請求項 7 記載の暗号通信センター装置。

【請求項 9】 前記暗号通信端末から前記アルゴリズム復号化鍵を要求された場合に、送信すべきアルゴリズム復号化鍵を暗号化し、この暗号化されたアルゴリズム復号化鍵を前記送信する情報として前記暗号化・復号化手段に入力する鍵暗号化手段を備えたことを特徴とする請求項 7 又は 8 記載の暗号通信センター装置。

【請求項 1 0】 前記鍵暗号化手段は、送信相手の暗号通信端末が固有に備える鍵により前記アルゴリズム復号化鍵を暗号化することを特徴とする請求項 7 乃至 9 のうち何れか一項に記載の暗号通信センター装置。

【請求項 1 1】 2 以上の前記請求項 1 乃至 6 のうち何れか一項に記載の暗号通信端末が設けられた暗号通信システム。

【請求項 1 2】 1 以上の前記請求項 1 乃至 6 のうち何れか一項に記載の暗号通信端末と前記請求項 7 乃至 1 0 のうち何れか一項に記載の暗号通信センター装置とが設けられた暗号通信システム。

【請求項 1 3】 暗号通信における情報送受信の一方となる暗号通信装置に用いられるプログラムであって、

前記暗号通信に用いる暗号アルゴリズムを 1 種類以上格納させるとともに、指定された暗号アルゴリズムを出力させる暗号アルゴリズム格納手段と、

前記暗号アルゴリズムに対応した暗号通信用の鍵を格納させるとともに、指定された鍵を出力させる鍵情報格納手段と、

前記暗号通信において何れの暗号アルゴリズム及び鍵を使用するかを、前記暗号アルゴリズム格納手段及び前記鍵情報格納手段に対してそれぞれ指定させる制御手段と、

前記暗号アルゴリズム格納手段に対して指定された暗号アルゴリズム及び前記鍵情報格納手段に対して指定された鍵によって、受信した暗号情報を復号化させ、又は、送信する情報を暗号化させる暗号化・復号化手段とを有するプログラムを記憶したコンピュータ読み取り可能な記憶媒体。

【請求項 1 4】 前記暗号アルゴリズム格納手段は、暗号化された暗号アルゴリズムを格納させるとともに、

前記暗号化された暗号アルゴリズムを、アルゴリズム復号化鍵によって復号化させる暗号アルゴリズム復号化手段を有するプログラムを記憶した請求項 1 3 記載の記憶媒体。

【請求項 1 5】 前記制御手段は、前記暗号アルゴリズム格納手段に格納させる何れかの暗号アルゴリズムについての送信要求を受けた場合に、当該要求暗号アルゴリズムを出力させるよう前記暗号アルゴリズム格納手段に指令させ、



前記暗号化・復号化手段は、前記要求暗号アルゴリズムを前記送信する情報として暗号化させるプログラムを記憶した請求項 1 3 又は 1 4 記載の記憶媒体。

【請求項 1 6】 通信相手から前記アルゴリズム復号化鍵を要求された場合には、該当するアルゴリズム復号化鍵を要求元への前記送信する情報として前記暗号化・復号化手段に入力させることプログラムを記憶した請求項 1 4 又は 1 5 記載の記憶媒体。

【請求項 1 7】 前記アルゴリズム復号化鍵にて暗号化された暗号アルゴリズムを複数種類格納させる更新用暗号アルゴリズム格納手段と、

通信相手から前記アルゴリズム復号化鍵を要求された場合には、該当するアルゴリズム復号化鍵を要求元への前記送信する情報として前記暗号化・復号化手段に入力させる手段とを有し、

前記制御手段は、前記暗号通信端末から暗号アルゴリズムを要求された場合には、前記更新用暗号アルゴリズム格納手段に対して要求暗号アルゴリズムを前記送信する情報として出力させるよう指令させるプログラムを記憶した請求項 1 4 記載の暗号通信センター装置。

【発明の詳細な説明】

【0 0 0 1】

【発明の属する技術分野】

この発明は暗号通信端末、暗号通信センター装置、暗号通信システム及び記憶媒体、更に詳しくは複数の暗号アルゴリズムが使用可能であり、かつ新規暗号アルゴリズムを安全かつ効率よく登録し使用可能である部分に特徴のある暗号通信端末、暗号通信センター装置、暗号通信システム及び記憶媒体に関する。

【0 0 0 2】

【従来の技術】

現在、ネットワークに接続された種々の機器には機密保持のために暗号化技術が組み込まれている。この組み込まれた暗号化技術を用いることで、ネットワークを介する電子商取引やコンテンツ配信事業等が盛んに行われようとしている。それらの業務は組み込まれている暗号化技術の安全性のもとに成り立っているものであり、このような背景から安全かつ効率の良い暗号アルゴリズムの設計に関

する研究が盛んに行われている。

【 0 0 0 3 】

しかしながら、暗号化技術を組み込んだ従来のシステムでは、規格標準化等によりシステム仕様が一度決まってしまうと、それと同時に、システムで使用する暗号方式が固定されてしまう。したがって、システムのセキュリティレベルも固定されることになる。

【 0 0 0 4 】

一方、安全な暗号アルゴリズムの設計に関する研究と同時に暗号アルゴリズムの安全性の評価のために暗号アルゴリズムの解読法の研究も盛んに行われている。したがって、システムで使用している暗号方式が解読されるといったことも現実には起こりうることである。

【 0 0 0 5 】

このようにシステムで使用している暗号方式が破られてしまった場合には、暗号方式を更新しない限り、当該システムをそのまま使用することができなくなる。すなわち安全なネットワーク通信を継続するには、システムの暗号方式を更新する必要が生じる。

【 0 0 0 6 】

【発明が解決しようとする課題】

しかしながら、ネットワークを介しての暗号方式更新は、秘密情報の外部への流出等の安全性の面で問題がある。一方、ネットワークを介さない変更では、システムのすべての機器に一台づつに暗号方式変更を加えなければならず、効率的な変更が不可能である。

【 0 0 0 7 】

本発明は、このような実情を考慮してなされたもので、その第 1 の目的は、暗号アルゴリズムを選択的に暗号通信を行うことができる暗号通信端末、暗号通信センター装置、暗号通信システム及び記憶媒体を提供することにある。

【 0 0 0 8 】

また、第 2 の目的は、新規暗号アルゴリズムをネットワークを介して安全かつ効率よく登録し、さらに登録したアルゴリズムを使用状態とすることができる暗

号通信端末、暗号通信センター装置、暗号通信システム及び記憶媒体を提供することにある。

【0 0 0 9】

【課題を解決するための手段】

上記課題を解決するために、請求項 1 に対応する発明は、暗号通信における情報送受信の一方となる暗号通信端末において、暗号通信に用いる暗号アルゴリズムを 1 種類以上格納するとともに、指定された暗号アルゴリズムを出力する暗号アルゴリズム格納部と、暗号アルゴリズムに対応した暗号通信用の鍵を格納するとともに、指定された鍵を出力する鍵情報格納部と、暗号通信において何れの暗号アルゴリズム及び鍵を使用するかを、暗号アルゴリズム格納部及び鍵情報格納部に対してそれぞれ指定する制御手段と、暗号アルゴリズム格納部に対して指定された暗号アルゴリズム及び鍵情報格納部に対して指定された鍵によって、受信した暗号情報を復号化し、又は、送信する情報を暗号化する暗号化・復号化手段とを備えた暗号通信端末である。

【0 0 1 0】

本発明はこのような手段を設けたので、暗号アルゴリズムを選択的に暗号通信を行うことができる。これにより、より安全な暗号方式を選択して暗号通信を行うことができる。

【0 0 1 1】

次に、請求項 2 に対応する発明は、請求項 1 に対応する発明において、暗号アルゴリズム格納部は、暗号化された暗号アルゴリズムを格納するとともに、暗号化された暗号アルゴリズムを復号化する暗号アルゴリズム復号化手段を備えた暗号通信端末である。

【0 0 1 2】

本発明はこのような手段を設けたので、端末装置において暗号アルゴリズムの安全性を確保することができ、ひいては暗号通信の秘匿性を高めることができる。

【0 0 1 3】

次に、請求項 3 に対応する発明は、請求項 2 に対応する発明において、鍵情報

格納部は、暗号通信用の鍵の他、暗号化された暗号アルゴリズムを復号化する際に用いるアルゴリズム復号化鍵を格納する暗号通信端末である。

【 0 0 1 4 】

本発明はこのような手段を設けたので、請求項 2 に対応する発明と同様に暗号アルゴリズムを第三者から守ることができる。

【 0 0 1 5 】

次に、請求項 4 に対応する発明は、請求項 1 ～ 3 に対応する発明において、鍵情報格納部は、暗号化された鍵を格納するとともに、暗号化された鍵を復号化する鍵情報復号化手段を備えた暗号通信端末である。

【 0 0 1 6 】

本発明はこのような手段を設けたので、暗号通信用の鍵やアルゴリズム復号化鍵を安全な状態で保持することができ、第三者に鍵を盗まれた場合でも、暗号アルゴリズム自体や通信鍵の安全性を確保することができ、ひいては暗号通信の秘匿性を高めることができる。

【 0 0 1 7 】

次に、請求項 5 に対応する発明は、請求項 1 ～ 4 に対応する発明において、制御手段は、暗号アルゴリズム格納部に格納する何れかの暗号アルゴリズムについての送信要求を受けた場合に、当該要求暗号アルゴリズムを出力するよう暗号アルゴリズム格納部に指令し、暗号化・復号化手段は、要求暗号アルゴリズムを送信する情報として暗号化する暗号通信端末である。

【 0 0 1 8 】

本発明はこのような手段を設けたので、新規暗号アルゴリズムをネットワークを介して安全かつ効率よく登録することができる。

【 0 0 1 9 】

次に、請求項 6 に対応する発明は、請求項 1 ～ 5 に対応する発明において、自己の通信相手が請求項 5 の暗号通信端末又は請求項 1 乃至 6 のうち何れか一項に記載の暗号通信端末を備える装置である場合に、当該通信相手に新たな暗号アルゴリズム及び又はこれに対応するアルゴリズム復号化鍵を要求し、その応答を暗号化・復号化手段にて復号化するとともに、要求した暗号アルゴリズムを受け取

った場合にはこれを暗号アルゴリズム格納部に格納し、要求したアルゴリズム復号鍵を受け取った場合にはこれを前記鍵情報格納部に格納する暗号通信端末である。

【 0 0 2 0 】

本発明はこのような手段を設けたので、新規暗号アルゴリズムをネットワークを介して安全かつ効率よく登録し、さらに登録したアルゴリズムを使用状態とすることができる。

【 0 0 2 1 】

次に、請求項 7 に対応する発明は、請求項 1 乃至 6 のうち何れか一項に記載の暗号通信端末を備えるとともに、通信相手からアルゴリズム復号化鍵を要求された場合には、該当するアルゴリズム復号化鍵を要求元への送信する情報として暗号化・復号化手段に入力する暗号通信センター装置である。

【 0 0 2 2 】

本発明はこのような手段を設けたので、アルゴリズム復号化鍵を集中的に管理し、端末からアルゴリズム復号化鍵の要求があったときにはこれを暗号通信でもって引き渡すことができる。

【 0 0 2 3 】

次に、請求項 8 に対応する発明は、請求項 7 に対応する発明において、請求項 5 記載の暗号通信端末を備える場合に、アルゴリズム復号化鍵にて暗号化された暗号アルゴリズムを複数種類格納する更新用暗号アルゴリズム格納部を備え、制御手段は、暗号通信端末から暗号アルゴリズムを要求された場合には、暗号アルゴリズム格納部に代え、更新用暗号アルゴリズム格納部に対して要求暗号アルゴリズムを送信する情報として出力するよう指令する暗号通信センター装置である。

【 0 0 2 4 】

本発明はこのような手段を設けたので、アルゴリズム復号鍵のみならず、暗号アルゴリズム自体も安全に要求端末に送信することができる。

【 0 0 2 5 】

次に、請求項 9 に対応する発明は、請求項 7 又は 8 に対応する発明において、

暗号通信端末からアルゴリズム復号化鍵を要求された場合に、送信すべきアルゴリズム復号化鍵を暗号化し、この暗号化されたアルゴリズム復号化鍵を送信する情報として暗号化・復号化手段に入力する鍵暗号化手段を備えた暗号通信センター装置である。

【0 0 2 6】

本発明はこのような手段を設けたので、暗号通信における暗号化に加えて元々の鍵自体も暗号化されるのでより安全にアルゴリズム復号化鍵を引き渡すことができる。

【0 0 2 7】

次に、請求項 1 0 に対応する発明は、請求項 7～9 に対応する発明において、鍵暗号化手段は、送信相手の暗号通信端末が固有に備える鍵によりアルゴリズム復号化鍵を暗号化する暗号通信センター装置である。

【0 0 2 8】

本発明はこのような手段を設けたので、要求を発した端末のみに対応する形でアルゴリズム復号化鍵を暗号化でき、安全性をより一層高めることができる。

【0 0 2 9】

次に、請求項 1 1 に対応する発明は、2 以上の前記請求項 1 乃至 6 のうち何れか一項に記載の暗号通信端末が設けられた暗号通信システムである。

【0 0 3 0】

本発明はこのような手段を設けたので、暗号アルゴリズムを選択的に暗号通信を行うことができる暗号通信システムを構築することができる。

【0 0 3 1】

次に、請求項 1 2 に対応する発明は、1 以上の請求項 1 乃至 6 のうち何れか一項に記載の暗号通信端末と請求項 7 乃至 1 0 のうち何れか一項に記載の暗号通信センター装置とが設けられた暗号通信システムである。

【0 0 3 2】

本発明はこのような手段を設けたので、暗号アルゴリズムを選択的に暗号通信を行うことができるとともに、新規暗号アルゴリズムをネットワークを介して安全かつ効率よく登録し、さらに登録したアルゴリズムを使用状態とすることが

できる暗号通信システムを構築することができる。

【 0 0 3 3 】

次に、請求項 1 3 に対応する発明は、請求項 1 に対応する発明をコンピュータに実現させるプログラムを記録した記憶媒体である。

【 0 0 3 4 】

この記憶媒体から読み出されたプログラムにより制御されるコンピュータは、請求項 1 の暗号通信端末として機能する。

【 0 0 3 5 】

次に、請求項 1 4 に対応する発明は、請求項 2 に対応する発明をコンピュータに実現させるプログラムを記録した記憶媒体である。

【 0 0 3 6 】

この記憶媒体から読み出されたプログラムにより制御されるコンピュータは、請求項 2 の暗号通信端末として機能する。

【 0 0 3 7 】

次に、請求項 1 5 に対応する発明は、請求項 5 に対応する発明をコンピュータに実現させるプログラムを記録した記憶媒体である。

【 0 0 3 8 】

この記憶媒体から読み出されたプログラムにより制御されるコンピュータは、請求項 5 の暗号通信端末として機能する。

【 0 0 3 9 】

次に、請求項 1 6 に対応する発明は、請求項 7 に対応する発明をコンピュータに実現させるプログラムを記録した記憶媒体である。

【 0 0 4 0 】

この記憶媒体から読み出されたプログラムにより制御されるコンピュータは、請求項 7 の暗号通信センター装置として機能する。

【 0 0 4 1 】

次に、請求項 1 7 に対応する発明は、請求項 8 に対応する発明をコンピュータに実現させるプログラムを記録した記憶媒体である。

【 0 0 4 2 】

この記憶媒体から読み出されたプログラムにより制御されるコンピュータは、請求項 8 の暗号通信センター装置として機能する。

【 0 0 4 3 】

【発明の実施の形態】

以下、本発明の実施の形態について説明する。

【 0 0 4 4 】

なお、各実施形態では、暗号化されたデータを  $E1(x)[y]$ 、 $E2(x)[y]$ 、 $E(z, x)[y]$  等と表す。ここで、 $x$  は暗号化に用いる鍵を表し、 $y$  は暗号化対象のデータを表し、 $z$  は暗号化に用いるアルゴリズムを表す。また、 $a | b$  は  $a$  と  $b$  の接続を表す。

【 0 0 4 5 】

(発明の第 1 の実施の形態)

図 1 は本発明の第 1 の実施の形態に係る暗号通信システムの一例を示す構成図である。

【 0 0 4 6 】

同図に示す暗号通信システムは、インターネットや LAN 等の種々のネットワーク 1 に暗号通信端末 2 (以下、単に端末 2 ともいう) 及び暗号通信センター装置 3 (以下、単にセンター 3 ともいう) が接続されて構成されている。各端末 2 間、及び端末 2 ~ センター 3 間ではネットワーク 1 を介して通信 (あるいは暗号通信) が実行可能に構成されている。

【 0 0 4 7 】

図 2 は暗号通信端末の構成例を示すブロック図である。

【 0 0 4 8 】

暗号通信端末 2 は、制御部 1 1、鍵情報格納部 1 2、暗号アルゴリズム格納部 1 3、暗号化・復号化部 1 4、鍵情報復号化部 1 5、暗号アルゴリズム復号化部 1 6 及び ID 格納部 1 7 から構成されている。この端末 2 は、CPU やメモリ等の計算機要素を備えた手段であり、プログラムに制御される CPU の動作により上記各機能手段を実現している。また、ネットワーク通信のために、図示しない通信装置を備えている。



【0 0 4 9】

一方、図 3 は暗号通信センター装置の構成例を示すブロック図である。

【0 0 5 0】

暗号通信センター装置 3 は、制御部 2 1、鍵情報格納部 2 2、暗号アルゴリズム格納部 2 3、暗号化・復号化部 2 4、端末鍵情報格納部 2 5、アルゴリズム復号化鍵格納部 2 6、鍵暗号化部 2 7、更新用暗号アルゴリズム格納部 2 8、端末権限管理部 2 9 及び I D 格納部 3 0 から構成されている。センター 3 は、端末 2 と同様、CPU やメモリ 等の計算機要素を備えた手段であり、プログラムに制御される CPU の動作により上記各機能手段を実現している。また、ネットワーク通信のために、図示しない通信装置を備えている。

【0 0 5 1】

ここでまず、暗号通信端末 2 の各構成要素について説明する。

【0 0 5 2】

制御部 1 1 は、各部 1 2 ～ 1 7 を制御することでデータの流れを制御し、例えば識別情報（I D）やメッセージ等を機能部 1 2，1 3，1 4 に与える。また、制御部 1 1 は、I D 情報を指定することで暗号通信の際に使用する秘密鍵や暗号アルゴリズムを選択するようになっている。

【0 0 5 3】

I D 格納部 1 7 は、センター 3 及び端末 2 の I D や、アルゴリズム（A 1）の I D、更には鍵の I D 等、種々の I D を格納する。

【0 0 5 4】

鍵情報格納部 1 2 は、暗号化された鍵情報を格納しており、端末等の I D 及びアルゴリズム I D を入力されると、これらに対応しかつ暗号化された鍵情報を鍵情報復号化部 1 5 に出力する。

【0 0 5 5】

鍵情報復号化部 1 5 は、鍵情報格納部 1 2 から引き渡された鍵情報を自己の固有の秘密鍵で復号化し出力する。

【0 0 5 6】

暗号アルゴリズム格納部 1 3 は、暗号化されたアルゴリズムを格納しており、

アルゴリズムIDを入力されると、これに対応しかつ暗号化された暗号アルゴリズムを暗号アルゴリズム復号化部16に出力する。

【0057】

暗号アルゴリズム復号化部16は、鍵情報復号化部15から受け取った鍵を用いて暗号アルゴリズム格納部13から出力された暗号アルゴリズムを復号する。

【0058】

暗号化・復号化部14は、暗号アルゴリズム復号化部16により復号されたアルゴリズムを用い、鍵情報復号化部15にて復号化された通信用の鍵によってメッセージMを暗号化する。

【0059】

次に、暗号通信センター装置の各構成要素について説明する。

【0060】

制御部21は、各部22～30の動作を制御して情報の流れを制御するとともに、ID等に対応する機能部に与える。また、制御部12は、ID情報を指定することで暗号通信の際に使用する秘密鍵や暗号アルゴリズムを選択するとともに、端末2が更新要求する暗号アルゴリズムやその復号化鍵を選択するようになっている。

【0061】

鍵情報格納部22は、各端末2とセンター3間で暗号通信するための秘密鍵を格納するとともに、端末IDを受け取ると対応する秘密鍵を暗号化・復号化部24に出力する。

【0062】

暗号アルゴリズム格納部23は、種々の暗号アルゴリズムを格納しており、アルゴリズムIDを受け取ると、対応する暗号アルゴリズムを暗号化・復号化部24に出力する。

【0063】

端末鍵情報格納部25は、各端末の固有の秘密鍵を格納しており、端末IDを受け取ると、対応する端末の秘密鍵を鍵暗号化部27に出力する。

【0064】

アルゴリズム復号化鍵格納部 2 6 は、暗号化された各暗号アルゴリズムの復号化鍵を格納しており、アルゴリズム ID を受け取ると、対応する暗号アルゴリズムの復号化鍵を鍵暗号化部 2 7 に出力する。

【0 0 6 5】

鍵暗号化部 2 7 は、端末固有の秘密鍵によって暗号アルゴリズムの復号化鍵を暗号化し暗号化・復号化部 2 4 に出力する。

【0 0 6 6】

更新用暗号アルゴリズム格納部 2 8 は、端末 2 に与えるべき新たな暗号アルゴリズムを格納しており、アルゴリズム ID を受け取ると、これに対応しかつ暗号化された暗号アルゴリズムを暗号化・復号化部 2 4 に出力する。

【0 0 6 7】

暗号化・復号化部 2 4 は、鍵暗号化部 2 7 から出力されたアルゴリズム復号化鍵及び又は更新用暗号アルゴリズム格納部 2 8 から出力された暗号アルゴリズムを、暗号アルゴリズム格納部 2 3 からの暗号アルゴリズムを用い、鍵情報格納部 2 2 から受け取った鍵により暗号化する。

【0 0 6 8】

端末権限管理部 2 9 は、更新用暗号アルゴリズムやそのアルゴリズム復号化鍵を要求する端末が正当権限を有するものであるかをチェックし、正当権限を揺する場合のみ、上記各部 2 1～2 8 による処理を許可する。

【0 0 6 9】

ID 格納部 3 0 は、端末や、アルゴリズム、アルゴリズム復号鍵等の ID を格納しており、何れかの端末 2 から ID 取得要求があったときには、その ID を要求端末 2 に送信する。

【0 0 7 0】

次に、以上のように構成された本実施形態における暗号通信システムの動作について説明する。

【0 0 7 1】

まず、端末間暗号通信について説明する。

【0 0 7 2】

図4は端末間で暗号通信が行われる様子を示す図である。

【0073】

同図では、端末2*i*から端末2*j*へメッセージMが暗号アルゴリズムA1で暗号化されて送信される手順が示されている。

【0074】

この場合まず、送信先の端末2*j*の名前やメールアドレス等のID情報ID*j*と暗号通信の際使用する暗号アルゴリズムA1のID情報IDA1とが端末2*i*の制御部11によってID格納部17から取り出される。また、メッセージMが制御部11に入力される。すなわち制御部11は使用する暗号アルゴリズムの指定手段としても機能している。なお、端末2*i*及び2*j*は、予め必要なID情報をセンター3に請求し、当該センター3におけるID格納部30のID情報を取得している。

【0075】

メッセージMは制御部11から暗号化・復号化部14に出力される。同様に、IDA1は暗号アルゴリズム格納部に出力され、ID*j*及びIDA1が鍵情報格納部12に出力される。

【0076】

ここで、鍵情報格納部12においては入力されたID情報より、対応する鍵情報が取り出され、鍵情報復号化部15に出力される。すなわちID*j*により暗号化された秘密鍵E1(K*i*)[K*i j*]が出力され、IDA1によりアルゴリズム復号化鍵E1(K*i*)[KA1]が出力される。ここで、K*i j*は端末2*i*, 2*j*間で暗号通信を行うための鍵であって、例えばDESの共通鍵等が相当する。

【0077】

この暗号化された鍵情報は、鍵情報復号化部15においてパスワードやICカードに保存されている鍵などの端末固有の鍵情報K*i*によって復号化される。このうち、暗号化されたアルゴリズムA1の復号化鍵であるKA1は暗号アルゴリズム復号化部16へ、K*i j*は暗号化・復号化部14へそれぞれ出力される。

【0078】

一方、暗号アルゴリズム格納部 16 からは、制御部 11 から入力された ID 情報に基づいて暗号アルゴリズム復号化部 16 に対し暗号化された暗号アルゴリズム E2 (KA1) [A1] が出力される。

【0079】

この入力された暗号化された暗号アルゴリズムは、暗号アルゴリズム復号化部 16 においてアルゴリズム復号化鍵 KA1 によって復号化され、暗号化・復号化部 14 に対して暗号化アルゴリズム A1 として出力される。

【0080】

暗号化・復号化部 14 においては、入力されたメッセージ M、暗号アルゴリズム A1、秘密鍵 Kij によって送信するメッセージ M が暗号化される。

【0081】

こうして作成された暗号文 E (A1, Kij) [M] には、送信元端末を示す IDi と、この暗号通信で使用する暗号アルゴリズムの IDA1 が添付され、図示しない送信装置によりネットワーク 1 を介して端末 2j に送信される。

【0082】

この暗号通信を受け取った端末 2j においては、まず、制御部 11 から IDA1 が暗号アルゴリズム格納部 13 に出力され、IDi 及び IDA1 が鍵情報格納部 12 に出力される。

【0083】

この ID 情報が入力された情報格納部 12 より、鍵情報復号化部 15 に対して暗号化された秘密鍵 E1 (Kj) [Kij] 及びアルゴリズム復号化鍵 E1 (Kj) [KA1] が出力される。

【0084】

暗号化されたこれらの鍵情報はパスワードや IC カードに保存されている鍵などの端末固有の鍵情報 Kj によって鍵情報復号化部 15 において復号化され、このうち KA1 は暗号アルゴリズム復号化部 16 へ、また Kij は暗号化・復号化部 14 へそれぞれ出力される。

【0085】

一方、制御部 11 から暗号アルゴリズム格納部 13 に入力された ID 情報に基

づき、当該暗号アルゴリズム格納部 1 3 から暗号アルゴリズム復号化部 1 6 に対して暗号化された暗号アルゴリズム E 2 (K A 1) [A 1] が出力される。

【0 0 8 6】

暗号アルゴリズム E 2 (K A 1) [A 1] は、暗号アルゴリズム復号化部 1 6 においてアルゴリズム復号化鍵 K A 1 により復号化され、暗号化・復号化部に対しアルゴリズム A 1 として出力される。

【0 0 8 7】

暗号化・復号化部 1 4 においては、端末 2 i から受け取った暗号文 E (A 1, K i j) [M] が暗号アルゴリズム A 1 及び秘密鍵 K i j によって復号化され、メッセージ M が出力される。

【0 0 8 8】

このようにして、端末 2 i から端末 2 j への暗号アルゴリズム A 1 による暗号通信が実現されることになる。このとき、最初に与えるアルゴリズム I D は適宜変更可能であるので、端末 2 i, 2 j の双方が登録している暗号アルゴリズムであればこれを自在に変更できる。

【0 0 8 9】

次に、端末 2 が保持していない暗号アルゴリズムをセンター 3 から取得し、新たな暗号アルゴリズムを登録する登録（更新）手順について説明する。この更新手続きには暗号通信センター装置 3 から暗号アルゴリズム及びその復号鍵のすべてを取得する更新手順 # 1 と、暗号アルゴリズムは他の暗号通信端末 2 から取得し、その復号鍵はセンター 3 から取得する更新手順 # 2 とがある。ここでは、更新手順 # 1 を説明し、第 2 の実施形態で更新手順 # 2 を説明する。

【0 0 9 0】

図 5 は暗号アルゴリズム及びその復号鍵のすべてを暗号通信センター装置 3 から取得する更新手順 # 1 の処理を示す図である。

【0 0 9 1】

同図では端末 2 i がセンターに対し、新しい暗号アルゴリズム A 1' 及び暗号アルゴリズム A 1' に対する暗号アルゴリズム復号化鍵 K A 1' を要求する場合を示している。

## 【0092】

このためにまず、端末2 iからセンター3に、端末2 iのID情報ID i、更新する暗号アルゴリズムのID情報IDA 1'、更新の際使用する暗号アルゴリズムのID情報IDA 1が送信される。なお、ID情報IDA 1'等は事前に端末2 iにおいてセンター3から取得され、ID格納部17に格納されている。

## 【0093】

各ID情報を受け取った暗号通信センター装置3においては、受信情報が制御部21に読み込まれる。さらに、制御部21から端末権限管理部29への問合せが行われて端末2 iが暗号アルゴリズムを取得する権限を備えているかが確認される。必要な場合には、端末2 iは自己を証明する暗証情報等を送信し、その暗証情報等が端末権限管理部29での権限確認に用いられる。なお、権限確認された後に、制御部21への読み込みが行われてもよい。

## 【0094】

権限確認後、制御部21にて読み込まれた各IDについて、当該制御部21から暗号アルゴリズム格納部23に対してIDA 1が出力され、また、鍵情報格納部22に対しID iが出力される。さらに、端末鍵情報格納部25に対しID iが出力され、アルゴリズム復号化鍵格納部26に対しIDA 1'が出力され、更新用暗号アルゴリズム格納部28に対しIDA 1'が出力される。

## 【0095】

この制御部21からのID情報出力に対応し、まず、暗号アルゴリズム格納部23からは暗号化・復号化部24に対し暗号アルゴリズムA 1が出力される。また、鍵情報格納部22からは暗号化・復号化部24に対し鍵K c iが出力される。ここで、鍵K c iは、端末2 iとセンター3間で暗号通信を行うための共通秘密鍵（例えばDES用の鍵）である。

## 【0096】

さらに、入力されたID情報各々に対応し、端末鍵情報格納部25からは鍵暗号化部27に対して端末2 i固有の鍵K iが出力され、アルゴリズム復号化鍵格納部26からは鍵暗号化部27に対しアルゴリズムKA 1'用の鍵KA 1'が出力される。なお、暗号通信センター装置3は、端末権限管理部29に登録された

すべての暗号通信端末 2 の固有の鍵 ( $K_i$ ,  $K_j$  等) を保持している。

【0097】

鍵暗号化部 27 においては、入力された端末 2  $i$  固有の鍵  $K_i$  とアルゴリズム復号化鍵  $KA1'$  によって、鍵  $KA1'$  が鍵  $K_i$  で暗号化され、その暗号化結果として  $E1(K_i)[KA1']$  が暗号化・復号化部 24 に出力される。

【0098】

一方、入力された ID 情報に基づき、更新用暗号アルゴリズム格納部 28 から暗号化・復号化部 24 に対し  $E2(KA1')[A1']$  が出力される。なお、 $E2(KA1')[A1']$  は、端末 2  $i$  から要求された暗号アルゴリズム  $A1'$  が鍵  $KA1'$  によって暗号化されたものである。

【0099】

こうして暗号化・復号化部 24 に対しては、暗号アルゴリズム  $A1$ 、秘密鍵  $K_{ci}$ 、更新情報  $E1(K_i)[KA1']$  及び  $E2(KA1')[A1']$  が入力される。更新情報  $E1(K_i)[KA1']$  及び  $E2(KA1')[A1']$  は、暗号化・復号化部 24 において暗号アルゴリズム  $A1$  に基づいて秘密鍵  $K_{ci}$  により暗号化される。

【0100】

この作成された暗号文  $E(A1, K_{ci})[IDA1' | E1(K_i)[KA1'] | E2(KA1')[A1']]$  と、 $ID_c$  と、 $IDA1$  とがセンター 3 の通信装置によりネットワーク 1 を介して端末 2  $i$  に送信される。

【0101】

この暗号通信を受信した端末 2  $i$  においては、その受信情報が制御部 11 に読み込まれ、暗号アルゴリズム格納部 13 に対し  $IDA1$  が出力され、鍵情報格納部 12 に対し  $ID_c$  及び  $IDA1$  が出力される。

【0102】

鍵情報格納部 15 からは、入力された ID 情報に基づき、鍵情報復号化部 15 に対し暗号化された秘密鍵  $E1(K_i)[K_{ci}]$  及びアルゴリズム復号化鍵  $E1(K_i)[KA1]$  が出力される。

【0103】



この各暗号化された鍵情報が入力された鍵情報復号化部 12 においては、端末固有の鍵情報  $K_i$  によってこれらが復号化される。ここで鍵  $KA1$  は暗号アルゴリズム復号化部 16 へ秘密鍵  $K_{ci}$  は暗号化・復号化部 14 へそれぞれ出力される。

## 【0104】

一方、制御部 11 から  $IDA1$  を入力された暗号アルゴリズム格納部 13 からは、暗号アルゴリズム復号化部 16 に対し暗号化された暗号アルゴリズム  $E2(KA1)[A1]$  が出力される。これを受けた暗号アルゴリズム復号化部 16 において、鍵情報復号化部 15 から入力されたアルゴリズム復号化鍵  $KA1$  により暗号化された暗号アルゴリズム  $E2(KA1)[A1]$  が復号化され、暗号化・復号化部に対し  $A1$  が出力される。

## 【0105】

暗号化・復号化部 14 では、センター 3 から受け取った暗号文  $E(A1, K_{ci})[IDA1' | E1(K_i)[KA1'] | E2(KA1')[A1']]$  が、暗号アルゴリズム  $A1$  及び密鍵  $K_{ci}$  によって復号化される。この復号化が行われた結果、 $IDA1'$  と対応付けて鍵情報格納部 12 に  $E1(K_i)[KA1']$  が出力され、暗号アルゴリズム復号化部 13 に  $E2(KA1')[A1']$  が出力される。

## 【0106】

こうして、鍵情報格納部 12 及び暗号アルゴリズム復号化部 13 に対し、暗号アルゴリズム  $A1'$  の ID 情報に対応して、暗号化された鍵情報及び暗号化された暗号アルゴリズムが登録されることになる。したがって、以降、 $IDA1'$  を受けると、これらの各部 12 及び 13 はそれぞれ  $IDA1'$  についての情報を出力するようになる。

## 【0107】

上述したように、本発明の実施の形態に係る暗号通信端末は、制御部 11 にて使用すべき暗号アルゴリズムを指定し、これに対応して暗号アルゴリズム格納部 13、鍵情報格納部 12 及び暗号化・復号化部 14 を設けたので、複数の暗号アルゴリズムから通信毎にアルゴリズムを選択して暗号通信を行うことができ、解

読される可能性が高くなったアルゴリズムを用いないようにすることで通信の安全性を高めることができる。

## 【0108】

また、本実施形態の暗号通信端末では、暗号アルゴリズム自体を暗号化して暗号アルゴリズム格納部13に格納しているので、万一暗号アルゴリズムが盗まれた場合でも、そのアルゴリズムの解読や悪用を防止することができる。

## 【0109】

さらに、暗号通信用の鍵やアルゴリズム復号化鍵自体も暗号化がなされているので、これらの鍵が盗まれた場合の悪用を防止することができる。例えば暗号化されたアルゴリズム復号化鍵と暗号化された暗号アルゴリズムとが同時に盗まれても安全性は保持される。

## 【0110】

さらに、本実施形態の暗号通信端末では、新たな暗号アルゴリズム及びアルゴリズム復号化鍵を要求した場合に、その応答を復号し、それぞれを暗号アルゴリズム格納部13及び鍵情報格納部13に格納するようにしているので、新規暗号アルゴリズムをネットワークを介して安全かつ効率よく登録することができる。さらに一旦登録されると、次回からはアルゴリズムIDを指定するだけでその使用が可能になるため、取得したアルゴリズムを容易に使用可能状態とすることができる。

## 【0111】

また、本実施形態の暗号通信端末では、端末固有の鍵 $K_i$ 等の保管あるいは同鍵 $K_i$ 等を扱う鍵情報復号化部15に、ICカード等、内部構造を解析されにくい耐タンパー装置を用いるようにしたので、固有の鍵を不正に取得しようとする行為に対して高い防御力を発揮することができ、ひいては暗号アルゴリズムの不正流出を防ぐことができる。

## 【0112】

また、本実施形態の暗号通信センター装置は、更新用暗号アルゴリズム格納部26と、鍵情報格納部22を備え、要求された暗号アルゴリズム及びアルゴリズム復号化鍵を暗号化して要求端末に送信するようにしたので、新規暗号アルゴリ

ズムをネットワークを介して安全かつ効率的に配布することができる。

【0 1 1 3】

したがって、現在使用している暗号方式が破られてしまったような場合でも、すぐに新しい暗号方式を更新することができ、安全なネットワーク通信の継続を容易に実現することができる。

【0 1 1 4】

また、本実施形態の暗号通信センター装置は、各端末 2 が有する端末固有の鍵によってアルゴリズム復号化鍵を暗号化するようにしたので、万一配布したアルゴリズム復号化鍵が盗まれた場合でも、効果的にアルゴリズム復号化鍵の秘匿性を保持することができる。

【0 1 1 5】

なお、暗号通信端末同士からなる暗号通信システム、あるいはこれに暗号通信センター装置を加えた暗号通信システムにおいても、上記と同様な効果を得ることができる。

【0 1 1 6】

(発明の第 2 の実施の形態)

本実施形態では、第 1 の実施形態の暗号通信システムにおいて、端末 2 が保持していない暗号アルゴリズムを取得する他の登録（更新）手順について説明する。

【0 1 1 7】

本実施形態の暗号通信システムは、第 1 の実施形態における暗号通信システムと同様に構成されている。相違点は、返される暗号アルゴリズム及びアルゴリズム復号化鍵が異なる点である。このために、制御部 1 1 は、第 1 の実施形態と同様に構成される他、端末 2 が更新要求する暗号アルゴリズムを選択するようになっている。これらは構成上の相違というよりは、端末 2 から送信する ID 情報及び又は ID 情報送信先によって変わる動作上の相違である。なお、本実施形態では第 1 の実施形態と同一部分には同一符号を付して詳細説明を省略する。

【0 1 1 8】

以下、本実施形態の動作について説明するが、既に登録された暗号アルゴリズ

ムによる暗号通信は第1の実施形態と同様であるので省略し、新たに登録すべきアルゴリズムについて、第1の実施形態で説明した更新手順#1と異なる更新手順#2について説明する。

【0119】

図6は本発明の第2の実施の形態に係る暗号通信システムにおいて暗号アルゴリズムのみを他の暗号通信端末から取得する更新手順#2の処理を示す図である。

【0120】

ここでは更新手順#2における第1の手続きとして、まず、暗号アルゴリズムのみを他の暗号通信端末から取得する手続きについて説明する。

【0121】

端末2jは更新手順#1若しくは#2によって暗号アルゴリズムA1'を取得している。例えば端末2iが自己が保持しない暗号アルゴリズムA1'によって端末2jと通信しようとするとき、その通信に先立ち、まず、端末2iから暗号アルゴリズムA1'及びその復号化鍵の取得、登録が行われる。この登録処理は、端末2j及びセンター3のそれぞれに並行して各情報の取得要求がなされることで実現される。

【0122】

このために端末2iが端末2jに対し新しい暗号アルゴリズムA1'を要求する場合、まず、端末2iからIDi、更新する暗号アルゴリズムのID情報IDA1'及び更新の際使用する暗号アルゴリズムのID情報IDA1が端末2jに対して送信される。

【0123】

これらの情報を受け取った端末2jにおいては、当該受信情報が制御部11に読み込まれ、制御部11から暗号アルゴリズム格納部13にIDA1及びIDA1'が出力される。また、鍵情報格納部12に対しIDi及びIDA1が出力される。

【0124】

ID情報が入力された鍵情報格納部12からは鍵情報復号化部15に対し暗号

化された秘密鍵  $E 1 (K j)$   $[K i j]$  及びアルゴリズム復号化鍵  $E 1 (K j)$   $[K A 1]$  が出力される。さらに、鍵情報復号化部 1 5 では暗号化された鍵情報がパスワードや IC カードに保存されている鍵などの端末固有の鍵情報  $K j$  によって復号化され、鍵  $K A 1$  が暗号アルゴリズム復号化部へ鍵  $K i j$  が暗号化・復号化部へそれぞれ出力される。

【0 1 2 5】

一方、ID 情報が入力された暗号アルゴリズム格納部 1 3 からは、暗号アルゴリズム復号化部 1 6 に対し暗号通信用の暗号化された暗号アルゴリズム  $E 2 (K A 1)$   $[A 1]$  が出力される。さらに、暗号化・復号化部 1 4 に対し、端末 2 i に送信すべき暗号化された暗号アルゴリズム  $E 2 (K A 1')$   $[A 1']$  が出力される。

【0 1 2 6】

暗号アルゴリズム復号化部 1 6 では、入力された暗号化された暗号アルゴリズム  $E 2 (K A 1)$   $[A 1]$  がアルゴリズム復号化鍵  $K A 1$  によって復号化され暗号アルゴリズム  $A 1$  が取り出されて、暗号化・復号化部 1 4 に出力される。

【0 1 2 7】

暗号化・復号化部 1 4 においては、入力された暗号アルゴリズム  $A 1$ 、秘密鍵  $K i j$  によって更新情報  $E 2 (K A 1')$   $[A 1']$  が暗号化される。この暗号文  $E (A 1, K i j)$   $[I D A 1' | E 2 (K A 1') [A 1']]$  と  $I D j$  と  $I D A 1$  とが通信装置によってネットワーク 1 を介して端末 2 i に送信される。

【0 1 2 8】

この送信情報は端末 2 i にて受信され、当該受信情報が制御部 1 1 に読み込まれ、暗号アルゴリズム格納部 1 3 に対し  $I D A 1$  が出力される。また、制御部 1 1 からは鍵情報格納部 1 2 に対し  $I D j$  及び  $I D A 1$  が出力される。

【0 1 2 9】

入力された ID 情報に基づき、鍵情報格納部 1 2 からは鍵情報復号化部 1 5 に対し、暗号化された秘密鍵  $E 1 (K i)$   $[K i j]$  及びアルゴリズム復号化鍵  $E 1 (K i)$   $[K A 1]$  が出力される。

【0 1 3 0】

この入力された暗号化された鍵情報は、鍵情報復号化部 15 においてパスワードや IC カードに保存されている鍵などの端末固有の鍵情報  $K_i$  によって復号化される。この復号化された鍵のうち、鍵  $KA1$  は暗号アルゴリズム復号化部 16 へ出力され、端末間暗号通信用の鍵  $K_{ij}$  は暗号化・復号化部 14 へそれぞれ出力される。

## 【0131】

一方、暗号アルゴリズム格納部 13 からは、入力された ID 情報に基づいて暗号化された暗号アルゴリズム  $E2(KA1)[A1]$  が暗号アルゴリズム復号化部 16 に対し出力される。暗号アルゴリズム復号化部 16 においては暗号化された暗号アルゴリズム  $E2(KA1)[A1]$  がアルゴリズム復号化鍵  $KA1$  によって復号化され、その暗号アルゴリズム  $A1$  が暗号化・復号化部 14 に対し出力される。

## 【0132】

暗号化・復号化部 14 においては、端末  $2j$  から入力された暗号文  $E(A1, K_{ij})[IDA1' | E2(KA1')[A1']]$  が、暗号アルゴリズム  $A1$  及び秘密鍵  $K_{ij}$  によって復号化される。この復号化された情報は、暗号化された暗号アルゴリズム  $E2(KA1')[A1']$  であり、同情報は  $IDA1'$  と対応付けられて暗号アルゴリズム復号化部 13 に登録される。

## 【0133】

このようにして、新たな暗号アルゴリズム  $A1'$  が端末  $2i$  に登録されるが、このアルゴリズムを使用可能状態にするためには、当該情報  $E2(KA1')[A1']$  を復号化して  $A1'$  を取り出すための復号化鍵  $KA1'$  を取得する必要がある。この復号化鍵  $KA1'$  は各端末固有の秘密鍵により暗号化されているため、他の端末  $2j$  から取得することはできない。したがって、鍵の一括管理を行う暗号通信センター装置 3 に自己の固有の秘密鍵で暗号化したものを発行してもらう必要がある。

## 【0134】

そこで、次に、更新手順 #2 における第 2 の手続きとして、暗号アルゴリズム復号化鍵  $KA1'$  を暗号通信センター装置 3 から取得する手続きについて説明す

る。

【0135】

図7は暗号アルゴリズム復号化鍵を暗号通信センター装置から取得する更新手順#2の処理を示す図である。

【0136】

まず、端末2iからセンター3に対し、端末2iのID情報IDi、要求する暗号アルゴリズム復号化鍵のID情報IDKA1'及びこの暗号通信で使用される暗号アルゴリズムのID情報IDA1が送信される。

【0137】

この各ID情報を受信した暗号通信センター装置3では、まず、受信情報が制御部21に読み込まれた後、第1実施形態の更新手順#1と同様にして端末権限管理部29により権限確認が行われる。なお、権限確認された後に、制御部21への読み込みが行われてもよい。

【0138】

読み込まれた各ID情報について、制御部21から暗号アルゴリズム格納部23に対しIDA1が出力され、また、鍵情報格納部22に対しIDiが出力される。また、端末鍵情報格納部25に対しIDiが出力され、アルゴリズム復号化鍵格納部26に対しIDKA1'が出力される。

【0139】

この入力ID情報に対応し、暗号アルゴリズム格納部23からは暗号化・復号化部24に対し暗号アルゴリズムA1が出力される。また、鍵情報格納部22からは入力されたID情報より、暗号化・復号化部に対し、端末～センター間での暗号通信用の鍵Kciが出力される。端末鍵情報格納部25からは入力されたID情報より、鍵暗号化部27に対し端末2i固有の鍵Kiが出力される。さらにアルゴリズム復号化鍵格納部26からは入力されたID情報より、鍵暗号化部27に対し鍵KA1'が出力される。

【0140】

鍵暗号化部27ではアルゴリズム復号化鍵KA1'が入力された端末2i固有の鍵Kiにより暗号化され、その暗号化結果であるE1(Ki)[KA1']が

暗号化・復号化部 24 に出力される。この暗号結果が端末 2 i 専用に作成された暗号化されたアルゴリズム復号化鍵情報である。

【0141】

暗号化・復号化部 24 では、更新情報  $E1(Ki)$   $[KA1']$  が暗号アルゴリズム  $A1$  及び秘密鍵  $Kci$  によって暗号化される。その暗号結果である暗号文  $E(A1, Kci) [IDKA1' | E1(Ki) [KA1']]$  と  $IDc$  と  $IDA1$  とが通信装置によってネットワーク 1 を介して端末 2 i に送信される。

【0142】

この暗号通信は端末 2 i にて受信され、その受信情報が制御部 11 に読み込まれる。制御部 11 に読み込まれた情報のうち、 $IDA1$  が暗号アルゴリズム格納部 13 に出力され、また、鍵情報格納部 12 に対し  $IDc$  及び  $IDA1$  が出力される。

【0143】

$ID$  情報を入力された鍵情報格納部 12 からは鍵情報復号化部 15 に対し、 $ID$  に対応して暗号化された秘密鍵  $E1(Ki) [Kci]$  及びアルゴリズム復号化鍵  $E1(Ki) [KA1]$  が出力される。これを受けた鍵情報復号化部 15 においては、パスワードや IC カードに保存されている鍵などの端末固有の鍵情報  $Ki$  によって各鍵情報が復号化される。このうち、鍵  $KA1$  が暗号アルゴリズム復号化部 16 へ出力され、鍵  $Kci$  が暗号化・復号化部 14 へ出力される。

【0144】

一方、暗号アルゴリズム格納部 13 からは、入力された  $ID$  情報より、暗号アルゴリズム復号化部 16 に対し暗号化された暗号アルゴリズム  $E2(KA1) [A1]$  が出力される。

【0145】

この暗号化された暗号アルゴリズム  $E2(KA1) [A1]$  は、暗号アルゴリズム復号化部 16 においてアルゴリズム復号化鍵  $KA1$  により復号化され、その復号結果である暗号アルゴリズム  $A1$  が暗号化・復号化部 14 に出力される。

【0146】

暗号化・復号化部 14 においては、センター 3 から受信した暗号文  $E(A1,$



$K_{ci}$ ) [ $IDKA1' \mid E1(K_i)[KA1']$ ] が、暗号アルゴリズム  $A1$  及び秘密鍵  $K_{ci}$  によって復号化される。この復号  $E1(K_i)[KA1']$  は、 $IDKA1'$  に対応付けて鍵情報格納部 12 に登録される。

【0147】

上述したように、本発明の実施の形態に係る暗号通信システムは、第 1 の実施形態と同様な効果が得られる他、第 1 の実施形態で説明した更新手順 # 1 では新しい暗号アルゴリズムと暗号アルゴリズムを復号化するための鍵の両方ともをセンターに要求し、センターは要求された 2 つを端末 2 に送っているのに対し、更新手順 # 2 では、他の端末に新しい暗号アルゴリズム、センター 3 に対応するアルゴリズム復号化鍵を要求しており、手順 # 2 のほうがセンター 3 の負荷を減らすことができる。

【0148】

また、更新手順 # 2 の場合でも、暗号アルゴリズム送信処理及びアルゴリズム復号鍵送信処理が、端末及びセンターで並列して行われるので、手順 # 1 の場合と同様な時間でこれらを取得することができる。

【0149】

なお、本発明は、上記各実施の形態に限定されるものでなく、その要旨を逸脱しない範囲で種々に変形することが可能である。

【0150】

例えば各実施形態では、各端末 2 が保持し、また、センター 3 が管理する全端末 2 の固有の鍵  $K_i$ 、 $K_j$  等を DES 等で用いられる共通秘密鍵の場合で説明した。しかし、本発明はこのような場合に限られるものではない。例えば RSA 等の公開鍵方式を用い、各端末 2 が秘密鍵を保持し、センター 3 では公開鍵を保持するようにしてもよい。例えばセンター側での  $K_i$  は公開鍵となり、端末側の  $K_i$  は秘密鍵となる。

【0151】

また、各実施形態で説明したセンター 3 においては、暗号アルゴリズム復号化部 16 や鍵情報復号化部 15 を備えていないが、これらをセンター 3 に備え、また、通信に用いる暗号アルゴリズムや鍵も暗号化して格納し、端末 2 と同一の暗

号通信機能を持たせるようにしてもよい。つまり、センター 3 側の通信機能はその秘密保持力の強さや外部からのアクセス環境等の種々の状況に応じて適宜な者とすることができる。

【0152】

また、実施形態では、LAN や WAN、あるいはインターネット等を介して端末 2 間あるいはセンター 3 ～端末 2 間で暗号通信する場合で説明したが、本発明の適用範囲はこのような場合に限られるものではない。

【0153】

例えば LAN や WAN として用いる場合であっても、他人同士での通信ばかりでなく、同一企業内の企業内情報管理システムに適用させることができる。企業内といえども権限無き者に対しては情報を公開すべきでない場合も多いからである。また、メールシステムに本発明を適用させるのも効果的である。

【0154】

さらに、実施形態における各端末 2 をファックス送受信装置とし、ファックス間で暗号通信を行う場合に本発明を適用することができる。電話回線といえども盗聴されることがあるからこれに対応するものである。この場合、容易に暗号方式を変更でき、一旦構築されたファックス網を有効活用できる。さらに、携帯電話や PHS 等を本発明にいう端末 2 としてもよい。

【0155】

また、ケーブルテレビや衛星テレビ、例えば BS 放送のスクランブルを暗号と考えたときに、このスクランブルが破られたときに、迅速かつ効果的に新たなスクランブルに変更することができる。このときには、BS チューナが端末 2 に相当し、また、放送発信側は端末 2 とセンター 3 を兼ねることになる。

【0156】

同様に、IT ビジョンや双方向テレビ等にも適用可能である。このような場合にはセットトップボックスが端末 2 に相当し、放送側のシステムが端末 2 とセンター 3 を兼ねる。

【0157】

なお、上記の例でもわかるように、本発明では、端末 2 間や端末 2 ～センター

3間におけるデータ伝送回線は有線のものに限らず、無線でもよい。

【0158】

さらに、本発明でいう端末は、いわゆる計算機装置単体のみにその機能がすべて保持されている場合に限定されるものではない。例えば実施形態で説明した発明を構成する機能が、サーバ計算機やその他の計算機に分散して設けられているような場合でも、単一の計算機装置にこだわらずにこれらの機能を集めたものが本発明でいう端末である。

【0159】

なお、実施形態に説明した装置は、記憶媒体に格納したプログラムをコンピュータに読み込ませることで実現させることができる。

【0160】

ここで本発明における記憶媒体としては、磁気ディスク、フロッピーディスク、ハードディスク、光ディスク（CD-ROM、CD-R、DVD等）、光磁気ディスク（MO等）、半導体メモリ等、プログラムを記憶でき、かつコンピュータが読み取り可能な記憶媒体であれば、その記憶形式は何れの形態であってもよい。

【0161】

また、記憶媒体からコンピュータにインストールされたプログラムの指示に基づきコンピュータ上で稼働しているOS（オペレーティングシステム）や、データベース管理ソフト、ネットワークソフト等のMW（ミドルウェア）等が本実施形態を実現するための各処理の一部を実行してもよい。

【0162】

さらに、本発明における記憶媒体は、コンピュータと独立した媒体に限らず、LANやインターネット等により伝送されたプログラムをダウンロードして記憶又は一時記憶した記憶媒体も含まれる。

【0163】

また、記憶媒体は1つに限らず、複数の媒体から本実施形態における処理が行われる場合も本発明における記憶媒体に含まれ、媒体構成は何らの構成であってもよい。

【0 1 6 4】

なお、本発明におけるコンピュータは、記憶媒体に記憶されたプログラムに基づき、本実施形態における各処理を実行するものであって、パソコン等の1つからなる装置、複数の装置がネットワーク接続されたシステム等の何れの構成であってもよい。

【0 1 6 5】

また、本発明におけるコンピュータとは、パソコンに限らず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本発明の機能を実現することが可能な機器、装置を総称している。

【0 1 6 6】

【発明の効果】

以上詳記したように本発明によれば、暗号アルゴリズムを選択的に暗号通信を行うことができる暗号通信端末、暗号通信センター装置、暗号通信システム及び記憶媒体を提供することができる。

【0 1 6 7】

また、本発明によれば、新規暗号アルゴリズムをネットワークを介して安全かつ効率よく登録し、さらに登録したアルゴリズムを使用状態とすることができる暗号通信端末、暗号通信センター装置、暗号通信システム及び記憶媒体を提供することができる。

【図面の簡単な説明】

【図 1】

本発明の第 1 の実施の形態に係る暗号通信システムの一例を示す構成図。

【図 2】

暗号通信端末の構成例を示すブロック図。

【図 3】

暗号通信センター装置の構成例を示すブロック図。

【図 4】

端末間で暗号通信が行われる様子を示す図。

【図 5】

暗号アルゴリズム及びその復号鍵のすべてを暗号通信センター装置 3 から取得する更新手順 # 1 の処理を示す図。

【図 6】

本発明の第 2 の実施の形態に係る暗号通信システムにおいて暗号アルゴリズムのみを他の暗号通信端末から取得する更新手順 # 2 の処理を示す図。

【図 7】

暗号アルゴリズム復号化鍵を暗号通信センター装置から取得する更新手順 # 2 の処理を示す図。

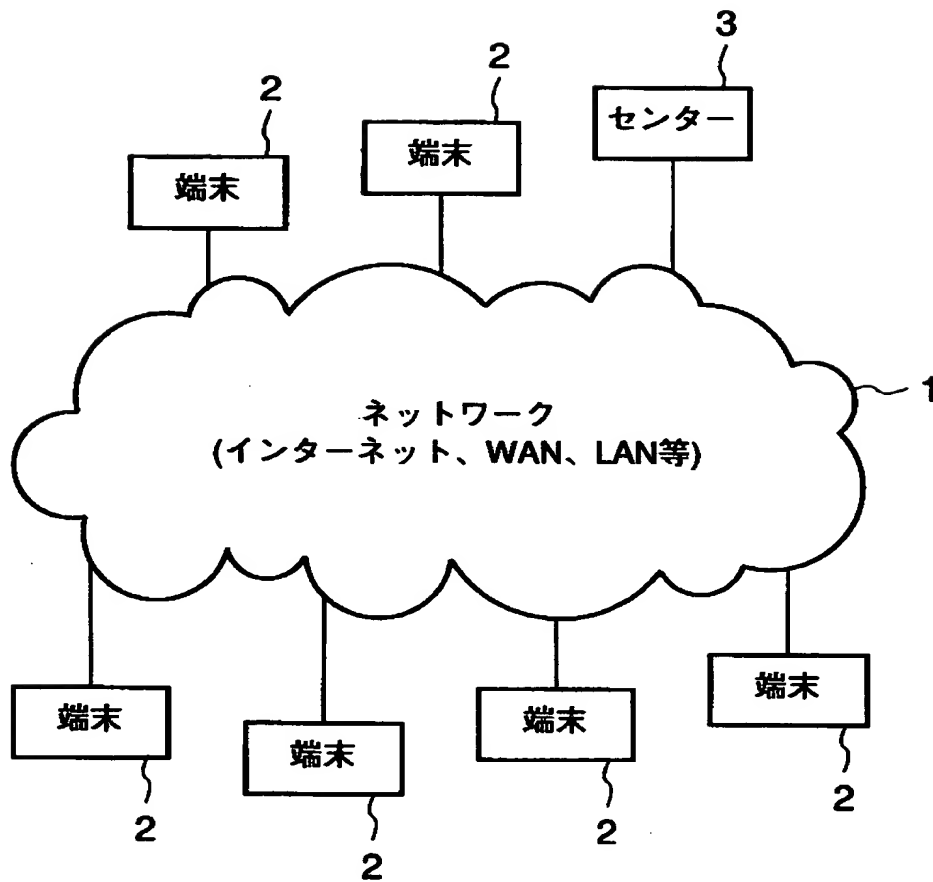
【符号の説明】

- 1 … ネットワーク
- 2 … 暗号通信端末
- 3 … 暗号通信センター装置
- 1 1 … 制御部
- 1 2 … 鍵情報格納部
- 1 3 … 暗号アルゴリズム格納部
- 1 4 … 暗号化・復号化部
- 1 5 … 鍵情報復号化部
- 1 6 … 暗号アルゴリズム復号化部
- 1 7 … I D 格納部
- 2 1 … 制御部
- 2 2 … 鍵情報格納部
- 2 3 … 暗号アルゴリズム格納部
- 2 4 … 暗号化・復号化部
- 2 5 … 端末鍵情報格納部
- 2 6 … アルゴリズム復号化鍵格納部
- 2 7 … 鍵暗号化部
- 2 8 … 更新用暗号アルゴリズム格納部
- 2 9 … 端末権限管理部
- 3 0 … I D 格納部

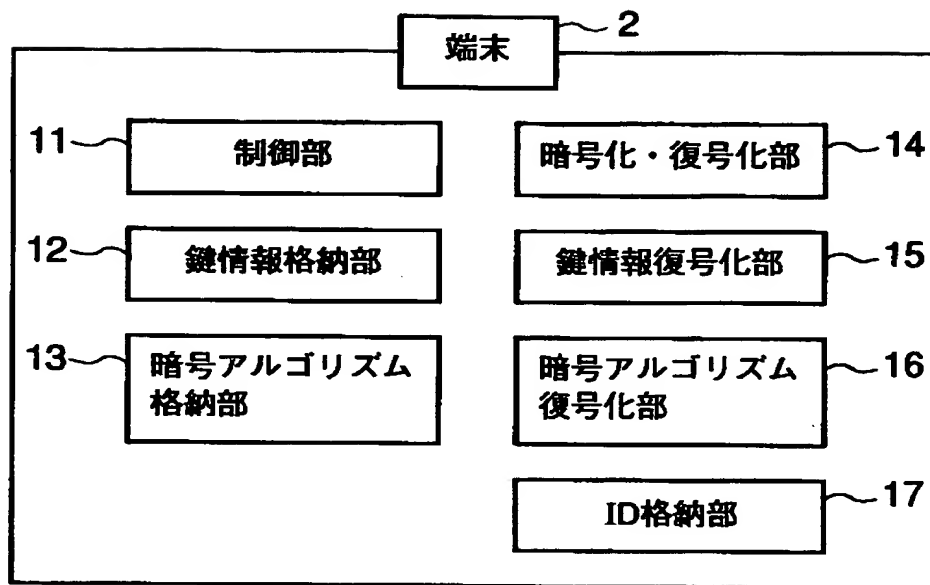
【書類名】

図面

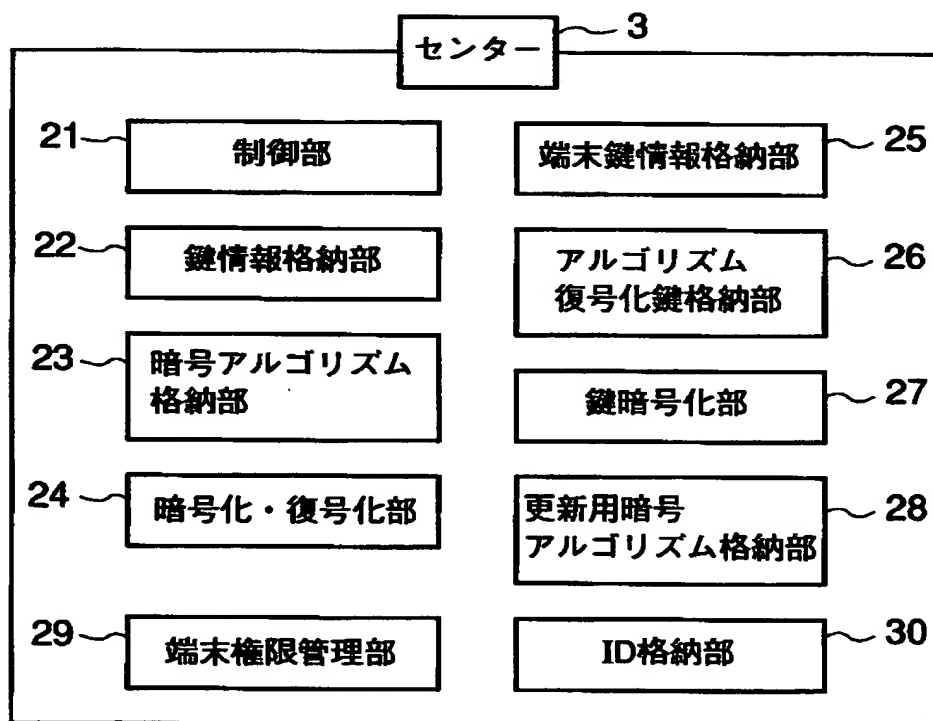
【図 1】



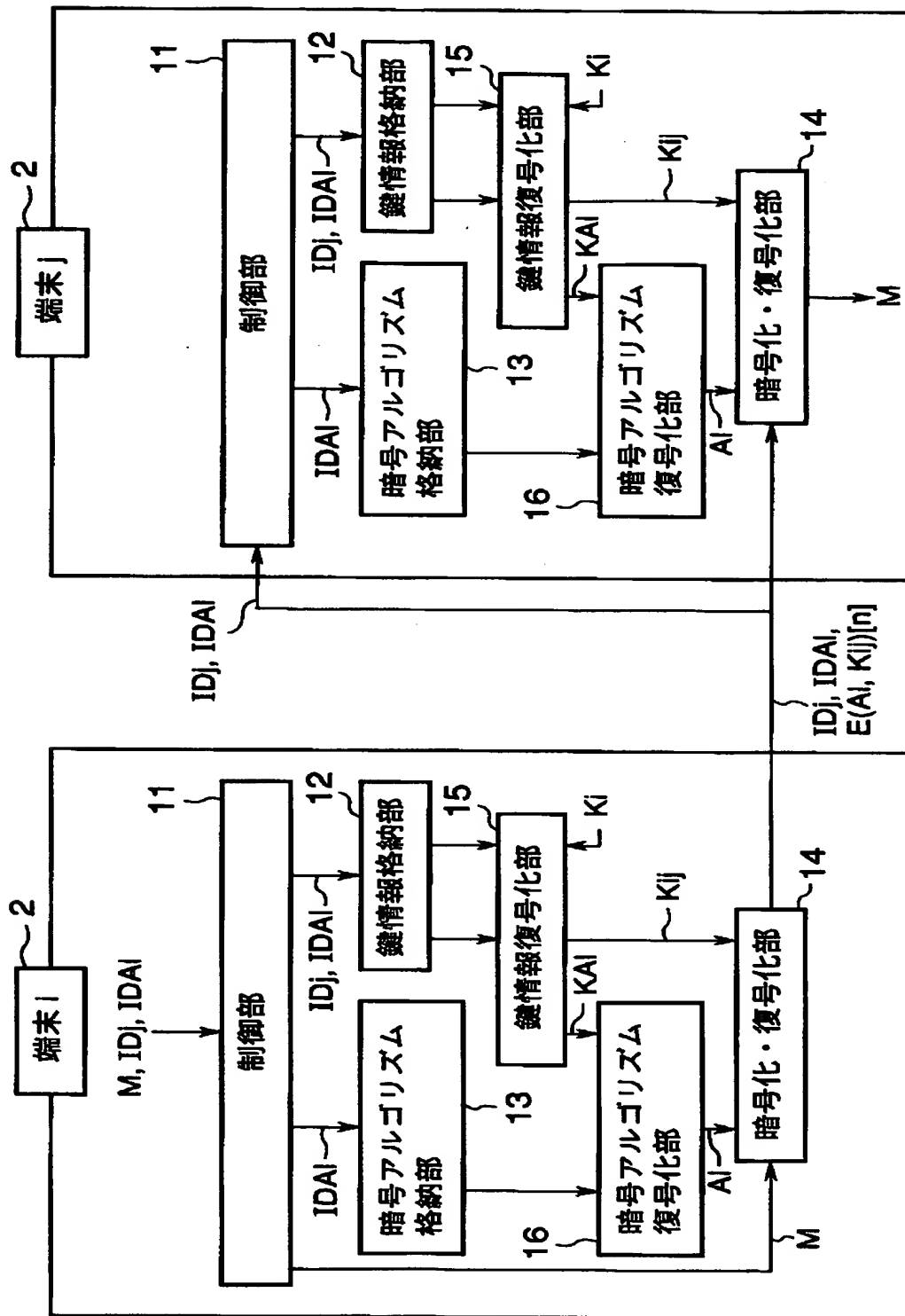
【図 2】



【図 3】

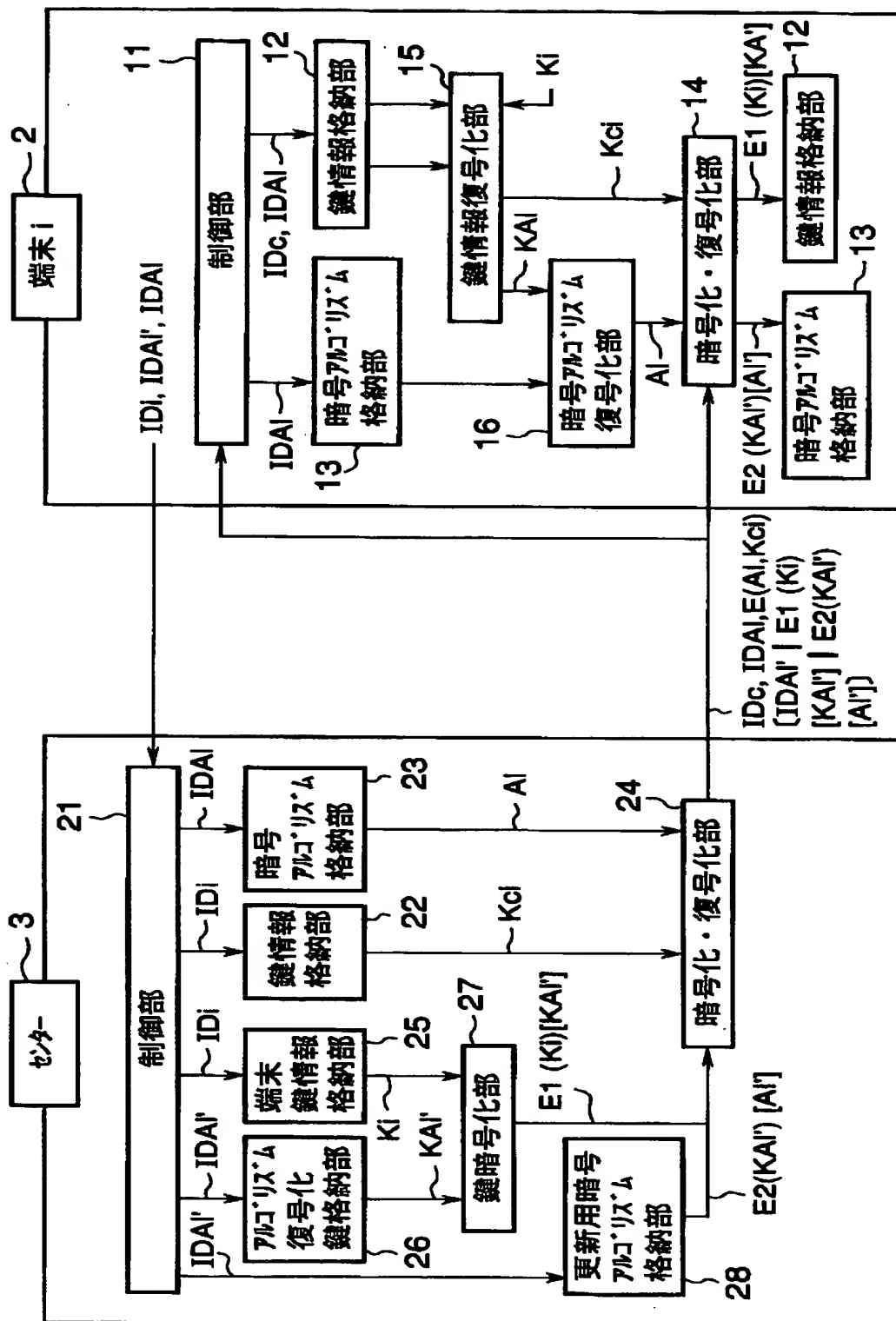


【図 4】

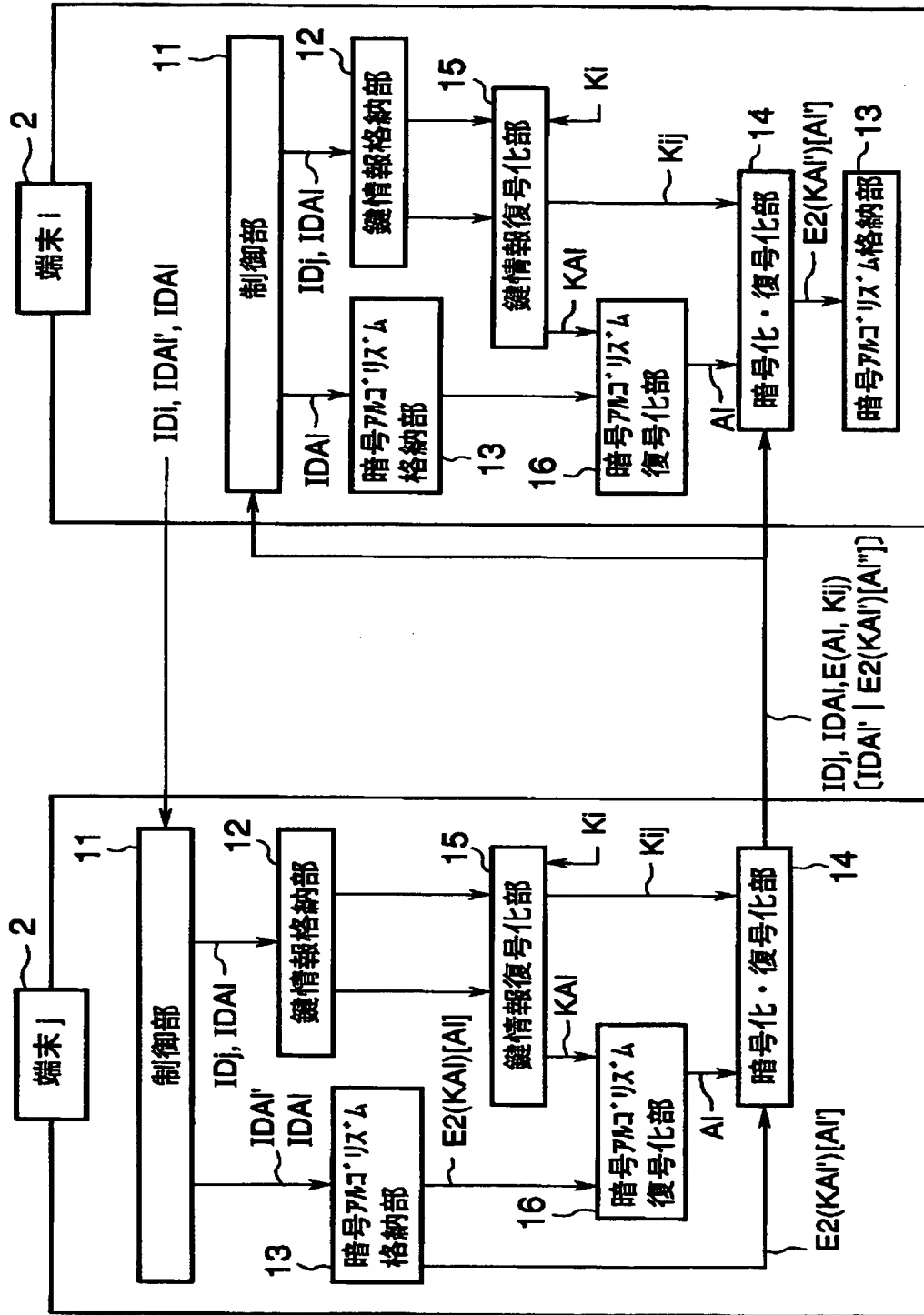




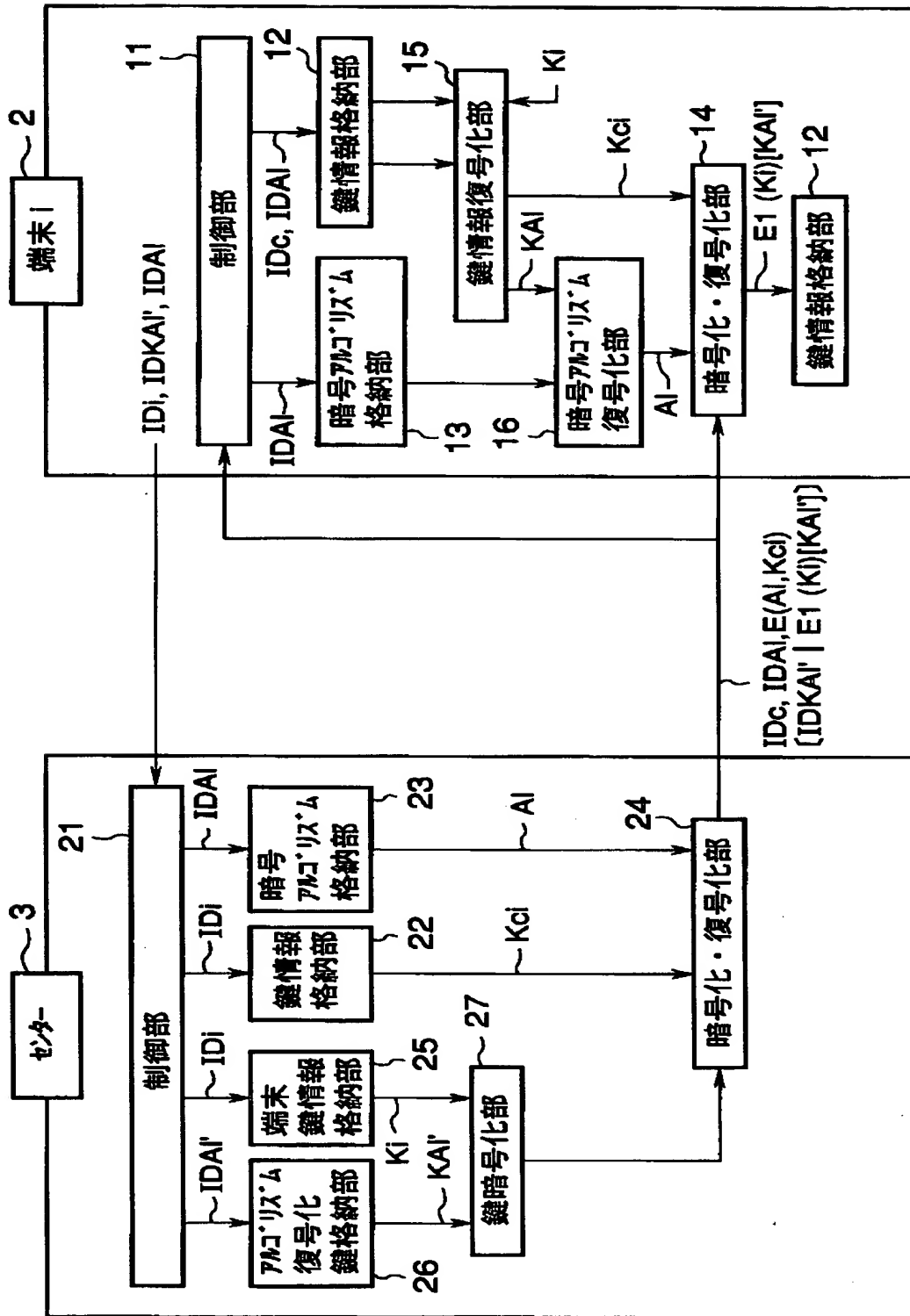
【図 5】



【図 6】



【図 7】



【書類名】                      要約書

【要約】

【課題】    暗号アルゴリズムを選択的に暗号通信を行うことができる。

【解決手段】    暗号通信での情報送受信の一方となる暗号通信端末 2 において、暗号通信に用いる暗号アルゴリズムを 1 種類以上格納するとともに、指定された暗号アルゴリズムを出力する暗号アルゴリズム格納部 1 3 と、暗号アルゴリズムに対応した暗号通信用の鍵を格納するとともに、指定された鍵を出力する鍵情報格納部 1 2 と、暗号通信において何れの暗号アルゴリズム及び鍵を使用するかを、暗号アルゴリズム格納部及び鍵情報格納部に対してそれぞれ指定する制御手段 1 1 と、暗号アルゴリズム格納部に対して指定された暗号アルゴリズム及び鍵情報格納部に対して指定された鍵によって、受信した暗号情報を復号化し、又は、送信する情報を暗号化する暗号化・復号化手段 1 4 とを備えた暗号通信端末。

【選択図】              図 4

出 願 人 履 歴 情 報

識別番号 [000003078]

1. 変更年月日 1990年 8月22日

[変更理由] 新規登録

住 所 神奈川県川崎市幸区堀川町72番地  
氏 名 株式会社東芝